



PLANO DE CONTINGÊNCIA DE NEGÓCIOS

Versão: 13/01/2020

1. OBJETIVO

Definir as bases, princípios e regras para contingências e continuidade de negócios da UJAY CAPITAL INVESTIMENTOS LTDA. (doravante a “UJAY”).

2. REVISÃO, ATUALIZAÇÃO E TESTES

Este PCN deverá ser **revisado e atualizado a cada 2 (dois) anos**, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

Sem prejuízo do parágrafo anterior, **este PCN será igualmente objeto de validação e testes a cada 12 (doze) meses.**

A revisão e validação do PCN fica a cargo do Comitê de Risco e *Compliance*.

3. PRINCÍPIOS E OBRIGAÇÕES

O PCN é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

Para identificação das posições e sistemas críticos, devem ser considerados os riscos a seguir, no caso de interrupção do processo:

- a) impacto financeiro** – situações em que a descontinuidade de negócios possa atingir as carteiras ou fundos sob gestão, ou a situação financeira e patrimonial da UJAY;
- b) impacto legal** – descontinuidade de negócios passível de gerar consequências legais aos fundos e carteiras sob gestão, seus cotistas, ou mesmo à própria UJAY;
- c) impacto de imagem** – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da UJAY perante seus clientes e/ou o público investidor;
- d) acidentes, casos fortuitos e força maior** – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da UJAY, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

4. ANÁLISE DE RISCOS POTENCIAIS E CLASSIFICAÇÃO

Esse Plano de Continuidade de Negócios tem como objetivo definir os procedimentos que deverão ser seguidos pela UJAY no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos (falta de energia elétrica, problema de acesso aos dados do servidor, queda da conexão à internet, impedimento do acesso físico ao escritório, queda da telefonia, etc.), determinando os procedimentos que deverão ser seguidos, em relação à contingência.

A UJAY adota a seguinte classificação de riscos, com as respectivas providências a serem tomadas:

Nível 1: baixa probabilidade de ocorrência e/ou de impacto nas atividades da UJAY, com monitoramento cotidiano para a sua prevenção;

Nível 2: riscos demandantes de atenção constante, com impacto potencial médio nas atividades da UJAY e necessidade de maior nível de controles preventivos;

Nível 3: riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades da UJAY, com adoção de rigorosos controles preventivos.

São exemplos de riscos de nível 3 as situações de falha de segurança/manutenção das instalações e equipamentos críticos da UJAY, que têm como medidas preventivas a manutenção de extintores, sprinklers, detectores de fumaça e treinamento da brigada de incêndio, além da operação/instalação de *nobreaks*, *firewalls* e controles de acesso às dependências, sistemas e arquivos da UJAY.

São exemplos de riscos de nível 2 a desatualização/falha de operação de softwares/equipamentos da UJAY, cujas medidas preventivas incluem a atualização e verificação/testes de sua efetividade, seja nas dependências da UJAY, seja na sua estrutura alternativa de contingência, bem como a manutenção de equipamentos para pronta reposição, operação ou substituição, de modo a sempre possibilitar a continuidade normal de suas atividades, mesmo em eventos de crise.

São exemplos de riscos de nível 1 situações não diretamente relacionadas à UJAY e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle

5. CONTROLES PREVENTIVOS (BACK UP E OUTROS)

PROCEDIMENTOS TECNOLÓGICOS



Diariamente, todos os arquivos localizados na rede de arquivos da UJAY são copiados, de maneira automática, para um *Hard Drive* externo. Pela norma interna, o *backup* se dará da seguinte forma:

(i) para a garantia do backup das informações da empresa, estas devem ser armazenadas nos servidores da rede corporativa;

(ii) não haverá garantia de *backup* para arquivos armazenados nas estações de trabalho (*desktops* ou *notebooks*);

(iii) o *backup* é armazenado no *Storage de Backup* local e realizado em local de contingência (*off-site* em *datacenter*);

(v) o *restore* de dados deve ser solicitado ao departamento de TI e será realizado de acordo com os procedimentos específicos do mesmo;

Além desse backup do servidor, a UJAY possui um processo de sincronização da pasta: U:\RISK\BackOffice_UJAY\INTERFACE\dropbox

Esta pasta contém os arquivos necessários para o funcionamento da UJAY no local de contingência e, em casos de utilização deste local, necessitaremos apenas baixar este arquivo do local de *backup* na internet.

CONTROLES E SALVAGUARDAS ADICIONAIS

- ✓ Controle de acesso às dependências da UJAY e do edifício;
- ✓ *Nobreaks* para atender o CPD e as posições de trabalho.
- ✓ A UJAY possui como local de contingência, localizado a aproximadamente 7 KM da sede, com 1 ramal de telefone e 1 notebook que possui as seguintes características:
 - Está preparado para acesso/recepção do banco de dados salvo no backup (Microsoft Sql Server);
 - Conexão de Internet rápida;
 - Acesso aos sistemas de cotações online (*Bloomberg, ValeBroker, Capital IQ* e *Broadcast, Pacote Microsoft Office*);
 - Local de contingência: Rua Alexandre Dumas, 1601 – Cj 68 – São Paulo

A chave e a senha do *notebook* ficam em poder do responsável por TI na UJAY.

Adicionalmente, os gestores e demais funcionários envolvidos nas funções necessárias para a continuidade dos negócios possuem dispositivos tecnológicos (*notebooks, desktops, smartphones, etc.*) configurados e de pleno acesso aos sistemas, senhas, etc. necessários para o exercício de suas funções de forma remota.

6. PROCEDIMENTOS DE CONTINGÊNCIA

Em casos de necessidade/contingência três pessoas deverão ser acionadas, estando presentes no local de contingência, ou com acesso remoto pleno a sistemas necessários para o exercício das atividades da UJAY, garantindo o funcionamento da empresa:

- ✓ **O responsável por risco e *backoffice*;**
- ✓ **Um dos gestores cadastrados no serviço *Bloomberg*;**
- ✓ **Outro gestor sócio da empresa.**

Além disso, um dos funcionários deverá monitorar o reestabelecimento do acesso a sede da empresa e a seus sistemas e ferramentas.

7. QUEDA DE ENERGIA NA SEDE

A UJAY disponibiliza em seu CPD um nobreak de 3 KVA, que tem o intuito de garantir a disponibilidade da operação da empresa em caso de falha de energia pela concessionária.

Abaixo, observa-se a autonomia do *nobreak* em diferentes situações:

- **35 min - Plena carga (todos os micros e equip.rack);**
- **2h e 10 min - Carga mínima (1 micro Bloomberg / 1 micro operação e CPD ativos / 2 monitores).**

Os procedimentos abaixo deverão ser seguidos em casos de queda de energia:

- **Após 5 minutos, para otimização, priorizar computador com terminal *Bloomberg* e outros suportes a gestão, desligando computadores que não sejam prioritários;**
- **Salvar todas as boletas do dia no arquivo TRADES.xlsm na pasta DROPBOX (botão *read* e salvar arquivo em U:\RISK\BackOffice_UJAY\INTERFACE\DROPBOX).**
- **Salvar todas as operações de aluguel do dia no arquivo ALUGUEIS.xlsm na pasta DROPBOX (botão *read* e salvar arquivo).**

Salvar em *pendrive* os seguintes arquivos:

- ***Backup* do Banco de Dados;**
- **UJAY.xlsm com as posições do dia (fazer a leitura através do botão *read*);**
- **TRADE.xlsm com os trades do dia (fazer a leitura através do botão *read*);**
- **Reportgen.xlsm com as últimas posições do fundo;**

Após 1h e 20 min preparar para procedimentos de **INACESSIBILIDADE DA SEDE**.

8. QUEDA DE CONEXÃO DE INTERNET



A UJAY possui duas conexões com a internet monitoradas por um firewall. Caso uma das conexões esteja com problema, a outra será utilizada. O sistema é monitorado através de um software chamado *WatchGuard System Manager*.

Procedimentos para queda de uma das conexões:

- **Automaticamente o sistema efetua a troca de conexão;**
- **Os usuários perceberão a queda da internet e deverão notificar a área de risco e *Compliance* ou o responsável por TI na UJAY;**
- **Estes verificarão qual das duas conexões falhou e deverão notificar a empresa provedora da conexão e demandar soluções;**
- **Os usuários continuarão trabalhando normalmente.**

Procedimento para queda das duas conexões:

- **Os usuários deverão notificar a área de risco e *Compliance* ou o responsável por TI na UJAY;**
- **A área de risco e *Compliance* deverá confirmar qual conexão não funciona;**
- **Verificando que nenhuma conexão funciona a área de risco e *backoffice* deverá verificar o funcionamento do firewall e do modem de cada provedor e reiniciá-los;**
- **Não retornando a conexão, a área de risco e *Compliance* deverá entrar em contato com a empresa de soluções em TI e com os provedores para demandar soluções.**

Caso a queda de conexão de internet seja de longo prazo, preparar para procedimentos de **INACESSIBILIDADE DA SEDE**.

9. QUEDA DE TELEFONIA

A UJAY possui linhas telefônicas digital e analógica além de um celular corporativo.

10. QUEDA DA LINHA DIGITAL VIVO

- Checar se o CPD está ligado e com o *led* da direita alternando entre vermelho e verde (se estiver somente piscando a luz vermelha há um problema na linha externa);
- Tentar reiniciar o modem da VIVO que está atrás do CPD (tirar o cabo de energia e religar depois de 30 seg);
- Se não retornar, acionar o atendimento da VIVO para efetuarem reparo (importante: sempre guardar o número de protocolo de atendimento).

Caso outras linhas deixem de funcionar:

- A área de risco e *Compliance* deverá ser notificada;



- Esta entrará em contato com a empresa responsável por prover o serviço de telefonia, solicitando soluções para o funcionamento normal da linha;
- As outras linhas deverão ser utilizadas enquanto a linha com problemas não retorne ao funcionamento normal.

11. INACESSIBILIDADE DA SEDE

Caso o acesso físico ao escritório da UJAY seja impedido por qualquer motivo, o local de contingência deverá ser utilizado para manter o funcionamento normal da empresa até que o acesso ao escritório seja novamente permitido ou um novo escritório esteja estruturado para o adequado funcionamento da empresa.

Na hipótese do acionamento da contingência os funcionários da UJAY deverão seguir os seguintes procedimentos:

Acionar o *notebook* e demais dispositivos de acesso remoto;

Na forma aplicável à função:

- Baixar/acessar os arquivos da pasta INTERFACE/*dropbox* cujo backup é arquivado no serviço DROPBOX.
- Baixar/acessar o banco de dados UJAY do backup do dia anterior (IBACKUP).
- Restaurar o banco de dados pela função *RESTORE* do Microsoft SQL Server Management Studio instalado e configurado na máquina;
- Instalar o *add-in* UJAY_V1.xlam;
- Adicionar no BD informações de operações do dia (caso existam) salvas no arquivo TRADE.xlsx;
- Habilitar/acessar os serviços de provedores de informações (inclusive informar a troca de máquina para o atendimento do *Bloomberg*);
- Continuar as atividades de operação do ponto em que foi interrompida.

12. ACESSO A INFORMAÇÕES RELEVANTES

Deverá ser mantida a disposição dos diretores e demais colaboradores uma lista (impressa e/ou digital) com as informações (nome, empresa, telefone e e-mail) de todos os integrantes da UJAY, das corretoras com as quais se realizam negócios, os clientes e os prestadores de serviço contratados.



Relatório de fechamento do dia anterior com todas as posições do fundo impresso e digital (relatório enviado por e-mail diariamente).

A UJAY também mantém listas de *Whatsapp* atualizadas com os contatos dos colaboradores para comunicação ágil nas hipóteses de acionamento de contingência.